Privacy Policy

Due Diligence Checking Limited ("**We**" or "**Us**") are committed to protecting and respecting your privacy.

This policy sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it. By agreeing to use our services you are accepting and consenting to the practices described in this policy. This policy shall be reviewed as part of our annual Data Protection review. We reserve the right to amend this policy at any time.

Contact & Company Details

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to our Data Protection Officer, Anish Bharakhda by email at contact@ddc.uk.net.

Our company details are as follows:

Registered Address:	1282a, Melton Road, Syston, Leicester, Leicestershire LE7 2HD
Telephone No:	0845 6443298 or 0116 260 3055
Company No:	04466929
VAT No:	799549932
ICO Registration No:	Z7242637

Information we collect from you

To complete the Disclosure application process, you will be required to enter personal data onto our website. This data meets the requirements set out by the **Relevant Authority** (Disclosure and Barring Service ("**DBS**"), Disclosure Scotland, AccessNI or any other applicable authority) to enable a request for criminal record information as per the level requested by your employer/endorsing body. Some of the information supplied by you for the Disclosure application process will also be used by us to carry out any additional pre-employment checks requested by your employing/endorsing organisation. In addition, we may ask you to supply additional information required by those pre-employment checks.

The request for a check is made by the employer/endorsing body acting as the "Data Controller" and we are acting as a "Data Processor" on behalf of this organisation. Definitions for Data Controller and Data Processor can be found in the UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018 (the "**UK GDPR**"). Standard Terms and Conditions which apply to the employer/endorsing body can be found on our website (https://www.ddc.uk.net/register).

The kind of information which we hold is listed in the Data Retention Matrix attached to this Privacy Policy.

The online process requires:

- an online form to be submitted and a declaration made relating to the type(s) of check requested;
- ID document information to be entered onto the system which meets the requirements of the Relevant Authority or other third-party providing checking services to us; and

- original ID documents to be examined by a named 'Document Checker' on the system (the Document Checker may be us or it may be your employer) OR a certified digital identity verification process to be carried out using an enabled smart phone with suitable data capture tools (e.g. a front facing camera of sufficient quality and an RFID/NFC antenna)*
- any discrepancies between form data, document data or obtained information to explained to the person validating the documents. They are under no obligation to accept this explanation and you may be asked to provide further evidence to confirm details.

*The employer/endorsing body must enable this feature with your application. If you choose to follow this process, then you will fill in an online form as described above, but you will then be prompted to switch to our mobile application ("**App**") by using the App to scan a QR code. You will then use our App to scan your ID documents, take a short video of yourself (which the App will convert to a digital image file), and submit the information to us. This will allow us to verify your identity digitally. Note that although we use third party technology in our App to support the processing of ID documents and verification of your appearance, we do not share any of your personal data with those technology providers – the information is sent only to our server. We may however need to verify your address or run additional anti-fraud checks using external credit reference agency checks or third-party suppliers. We are unable to accept any digital identity processes carried out by third-parties with whom we do not have a contractual relationship or processing agreement.

The paper-based process requires the same information in paper form instead.

On receipt of your completed form, we will transfer the data to the Relevant Authority using a secure connection e.g. e-Bulk or via post where applicable. If there are any errors or omissions on the form, we will telephone/email you to obtain the correct information, using the contact details you have provided.

For Standard and Enhanced checks, the Relevant Authority will issue one copy of the Disclosure Certificate document, which will usually be sent to the subject of the check. Where the document is 'clear', i.e. it shows no convictions or non-conviction information, we will be notified electronically and will relay this to the requesting organisation. If the document has content, we will be notified electronically that it has been issued and will relay this fact to the requesting organisation. You will then be contacted directly to arrange for the document to be inspected by the employer/endorsing body. If you dispute the information on the Disclosure you should contact the Relevant Authority directly. Your employer/endorsing body should also be notified. Where we receive a Disclosure Certificate document, we will liaise with you or the requesting organisation accordingly.

For Basic checks, a paper copy of the Disclosure Certificate document is issued to us by the Relevant Authority which is then sent to the requesting organisation for verification. The Disclosure Certificate is then sent to you if you have requested this or if the requesting organisation has arranged this.

For other pre-employment checks your personal data will be verified against other sources of information available to us. Where you have provided contact details for third parties e.g. referees or educational establishments, we will use these details to verify the information provided to us by you or your employer/endorsing body. We may also obtain information from independent sources as part of the verification process. Any references or confirmations obtained from third parties will be transferred to your employer/endorsing body. This may include any flags or concerns raised where information provided does not match another data

source obtained. Any decisions to raise a flag or concern are taken by our fully trained Case Workers and are not automated decisions. Some types of pre-employment information will show as a flag on the system; for example previous employment with a business no longer trading.

Some Regulatory Bodies offer a service where existing certificates can be validated with the original source to confirm if that issued document is still accurate. To undertake this process, you will be required to enter details of your previous document, and then present this with your original identity documents to ensure personal details are current. The regulatory body will not relay the details of the original certificate for re-review, but will advise if this is still current or if anything has changed. There is no obligation for an organisation to accept a previous certificate, and undertake identity validation steps, and they may require a new application to meet with their policies or processes.

What your information will be used for

All data submitted to us is handled in accordance with the Relevant Authority's guidelines and the UK GDPR. The personal data which we hold in any format relating to you will only be used by us for the purpose for which it has been provided or which you have consented to e.g. obtaining a Disclosure, other pre-employment check or verifying your identity digitally.

We will retain your personal data in accordance with the Data Retention Matrix attached to this policy and as follows: -

- Personal form data is submitted to the Relevant Authority for the purposes of a Disclosure check. Form data is deleted from our systems 30 days after the employment decision has been made. We keep records of your contact information, date of birth and other information necessary to demonstrate to the Relevant Authority that a compliant process has been followed for 7 years (or longer if required by the Relevant Authority or otherwise). However, the DBS (which aligns to Home Office standards for retention and disposal of records) is currently retaining some records indefinitely as due to ongoing inquiries, they are required to suspend the deletion of certain records. We may therefore retain some records indefinitely in line with the DBS Data Retention Policy which can be found online at the following link: https://www.gov.uk/government/publications/dbs-privacy-policies
- For the purpose of auditing paper applications, the application forms are kept for 7 years from the date of submission and are then securely destroyed.
- Identity document data and Digital Identity Verification data is used to verify your identity and ensure that the forms relevant to your application are fully completed, accurate and contain no conflicting information. Unless retained for a specific check type (e.g. Right to Work document check) form data is deleted from our systems 30 days after the employment decision has been made, or 90 days after a full pre-employment report has been seen by the employer/endorsing body. Some digital identity verification processes require images of the identity document, plus an image of the person presenting these to be retained on the report sent to the employer/endorsing body.
- The Disclosure and Barring Service require that details about the documents present for checking (including but not limited to document type, country of issue, any expiry

date, any reference numbers, and notes if there were any discrepancies discussed as part of the ID verification process) are retained for a minimum of 2 years.

- Access NI checks require copies of identity documents to be seen in advance and retained for 90 days after the completion of the application process.
- Disclosure Scotland checks require copies of identity documents and images of the person being checked to be seen in advance and retained for 6 months after the completion of the application process. Please note that compliance logs for higher level Disclosure Scotland applications must be retained by the submitting organisation (DDC) for 5 years and can only be deleted once the removal of interest processes have been completed. Applicants must ensure they respond to Disclosure Scotland requests appropriately or a new application may be required. Applicants must also ensure they make available their digital certificate to the requesting organisation through their Disclosure Scotland online portal. Failure to do so with the Disclosure Scotland required timeframes may result in the results being unobtainable and a new application required. Please check junk/spam folder regularly during your application process to ensure you do not miss any email notification from them in relation to issued certificates.
- For Standard and Enhanced checks, criminal record data is not routinely made available to Registered Bodies, such as ourselves. A single Disclosure Certificate is usually issued to you as the only copy of the information provided. We may be made aware if content is present, but not the content itself. We will inform a named person at the employer/endorsing body about the presence of content, but you must provide the Disclosure Certificate for review. However, in some circumstances we may receive a copy of the Disclosure Certificate and we will only use that information in accordance with this Privacy Policy.
- If we do receive any Disclosure Certificates from a Relevant Authority, they will be handled securely and in accordance with the service requested by the employer/endorsing body and the Relevant Authority's code of practice. This may include sending your certificate to the employer/endorsing body, at which point it becomes their responsibility to return it to you. You must contact us directly if you wish to receive this document and we will send this to you once the processing has been completed. Where we retain certificates (or other relevant documents such as PVG Scheme Update) this will be kept securely and shredded after 3 months. Certain circumstances allow for such documents to be retained for 12 months to meet external audit requirements for example CQC audits.
- Fingerprints are dealt with by your local police force through separate arrangements. We will assist in arranging the appointment but this will be the limit of our involvement.
- Third Party ID checks and credit checks are provided by a third-party provider to provide an alternative source of data to confirm your name/address/date of birth information. Suitable notices and consent for these services are obtained during the process, as required, or specifically collected by the employing/endorsing organisation. Third-party ID checks are available as part of a DBS check process where suitable identity documents are not available and you will be asked to declare that you do not hold such documents. This service is also available as part of the digital identity

service, to verify your declared address as an alternative to providing a physical document as evidence.

- Sanctions checks, identity checks and checks against international terrorism lists are provided by a third-party provider. The employing/endorsing organisation will specifically request this type of check upon you. In response to this request we will transfer data to them (name/date of birth/address) to allow them to complete their checks.
- International criminal record checks are provided by First Advantage Ltd. We will transfer your basic details to them (forename/surname/email address), where this type of check is requested, to enable you to log-in and consent to the particular country of the check. Depending on the requirements of the authority providing the results you may be asked to provide additional information. First Advantage Ltd have their own Privacy Policy detailing how they process data, which will include your rights under UK GDPR and the governing laws where the international check is to be processed. More information on the international transfer of data can be found on their website: https://privacy.sterlingcheck.com/
- Security challenge and responses taken to protect your form data. You choose a security question (from a list) and a response. Our agents will not know the full answer but will be available to offer a hint. If you do not know the answer to your security question, your form will reset to a blank form.
- Where your employer/requesting organisation requests your details are deleted from our system or has indicated you are no longer employed with them, we will delete your personal information (apart from information required to be kept for our records to demonstrate our legal compliance). Options are also available to anonymise data, however any such request must be made by the requesting organisation as the Data Controller.
- Any data provided by you may be used to independently verify information including but not limited to employment details, education references or personal references (as requested by the employer/requesting organisation). By providing these details you agree that we can make contact with the relevant employers, schools/universities or other organisations or individuals as part of our pre-employment check investigations.

Data sharing

Disclosure information stored by us will only be accessed by our Countersignatories and agents to:

- provide the requesting organisation with the number and issue date of the Disclosure;
- comply with any legal requirement, current or future, on us to give access to any information we hold on you e.g. Contact details, DOB, organisation requesting the Disclosure etc;
- where we receive the Disclosure, provide the requesting organisation with any content it may carry; or
- facilitate disposal of the Disclosure in a secure manner.

At no time will we use your personal data or any data on the Disclosure for any other purpose than as described above, or allow it to be copied, sampled or filed other than in the original form issued by the Relevant Authority.

We may however disclose your personal information to third parties in the following circumstances:

- In the event that we sell our business or assets, in which case we may disclose your personal data to the prospective buyer of our business or assets. For the avoidance of doubt, any disclosure under this exception will only be in relation to the sale of our business or assets as a whole or a certain part of our business. We will not sell your personal information for marketing or any other purposes.
- If we or substantially all of our assets are acquired by a third party, in which case personal data held by us will be one of the transferred assets.
- If we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or to protect the rights, property, or safety of us, our customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.
- If a specific check type requested by your employing/endorsing body is provided by a third party as set out below (e.g. an international criminal record check). As part of this process we may transfer the results of a check to a third party for translation services, to allow Case Workers to make results available.

In addition, as Data Controller, your employer/endorsing body can request to view the personal data which we hold and we are required by the UK GDPR to comply with such a request.

Standard and Enhanced Disclosures may contain sensitive information, which is protected by law under section 124 of The Police Act 1997. Protection of Vulnerable Groups checks in Scotland are protected under the relevant legislation in Scotland. The organisation that asked you to apply for a Disclosure has agreed to adhere to the relevant Code of Practice for use and dissemination of Disclosure information. Basic level checks contain information which is protected under the UK GDPR and other data protection legislation.

Third party providers:

We use the following third-party providers or partners for additional pre-employment checks and associated services where specifically requested by the employer/requesting organisation. Please note this does not include DBS, Access Northern Ireland nor Disclosure Scotland checks (which we process ourselves):.

- LexisNexis Risk Solutions Ltd.
- First Advantage Ltd.
- Experian Ltd.
- Equifax Ltd.
- Language Line Ltd.
- FaceTec, Inc.
- Higher Education Degree Datacheck (HEDD)
- Social Media Consulting Limited (SP Index)

Some of these third-party providers allow the secure submission of data using an Application Programming Interface (api) or similar connection. Where this is available DDC will build and test systems to ensure a robust and secure gateway connection. Connections to these

systems are commonly defined through documentation and best practice arrangements, against which DDC is audited. This may or may not include user access which is controlled through Single Sign On (SSO) systems as defined by the organisation requesting the checks. If this is the chosen set-up by the requesting organisation they should make you aware in advance.

Rights of access, correction, erasure, and restriction

Informing us of changes

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Your rights in connection with personal data

Under certain circumstances, by law you have the right to:

- **Request access to your personal data** (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data the data controller holds about you and to check that the data controller is lawfully processing it. The UK GDPR gives you the right to access information held about you. Within 30 days of receiving a subject access request in writing, the data controller will respond in writing to provide the details or advise on a reasonable delay, and reasons for that delay. The data controller may charge a reasonable fee for requests which are manifestly unfounded or excessive, particularly if they are repetitive.

- **Request correction** of the personal data that the data controller holds about you. This enables you to have any incomplete or inaccurate information the data controller holds about you corrected.

- **Request erasure** of your personal data. This enables you to ask the data controller to delete or remove personal data where there is no good reason for them continuing to process it. You also have the right to ask the data controller to delete or remove your personal data where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal data where the data controller is relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where the data controller is processing your personal data for direct marketing purposes.

- **Request the restriction** of processing of your personal data. This enables you to ask the data controller to suspend the processing of personal data about you, for example if you want the data controller to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal data to another party.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that the data controller transfers a copy of your personal data to another party, please contact the controller (your employer/requesting organisation). They do not have to comply with your request but they should explain why they believe they are entitled to refuse.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact your employer/requesting organisation. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law. Please note that where an application has already been completed, it is not possible to withdraw consent as the processing of your personal data has already occurred.

Information Security

We take information security very seriously and we hold several security and connection accreditations. We are ISO 27001 and ISO 9001 accredited and have also obtained PCI compliance to enable payment for applications through our secure online application portal. We use encrypted communications protocols and transmit data to Relevant Authorities via secure connections e.g. the e-Bulk communication system, which is part of the Criminal Justice Network operated by the Ministry of Justice and which is administered and approved by the DBS. More information on these accreditations and registrations can be found on our website www.ddc.uk.net/about-ddc/.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to us; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

Client Policies

In order to request a Disclosure an employer must provide you with their written policy on the employment of ex-offenders and their written policy on the storage, access, handling and usage of Disclosure information. A sample policy is made available to all employers/endorsing bodies through our website.

E-Commerce and Online Payments - Payment Conditions

In accordance with our merchant agreement with Elavon Financial Services, we adhere to the following conditions:

- All items are sold as per our merchant services agreement with Elavon, as stated on our Elavon application form.
- We do not sell items prohibited by Elavon.
- We retain responsibility for all transactions.
- Items of post are sent via Royal Mail Tracked Mail, or through normal postage methods. Other postage methods can be accommodated, but these must be specified by the client/applicant.
- Payment data is not stored by us (unless we are requested to do so), or used for any other purpose than to facilitate payment.
- All transactions are in GBP.

Refund Policy

Any payment to us is made on behalf of the employer/endorsing body and is composed of 2 parts; the disbursement fee that is sent directly to the Relevant Authority or other third-party provider, and the administration fee charged by us for the service carried out. Once the payment has been made for the application and you have entered data onto the form, the service is deemed to have been supplied and the administration fee is non-refundable.

If you wish to cancel an application that has already been paid for then this request must be made in writing and sent to Due Diligence Checking Limited, PO Box 6878, Syston, Leicester LE7 4ZR or emailed to contact@ddc.uk.net. We may seek further clarification to ensure that only genuine refund requests are received. We will be able to refund the Government fee paid prior to submission to the Relevant Authority. Once an application has been submitted to the Relevant Authority or other third-party provider, any applicable disbursement fee is non-refundable.

Complaints Policy

If you have a complaint about our service, you should contact us by email at contact@ddc.uk.net . Please include the word “Complaint” in the subject line of your email and provide full details of your complaint.

We will send you an acknowledgement of your complaint within 2 working days. Your complaint will then be passed to the appropriate person with authority to investigate your complaint. We aim to respond to your complaint as soon as possible and in any event within 10 working days of receiving your complaint.

You have the right to make a complaint at any time to the Information Commissioner's Office (“**ICO**”), the UK supervisory authority for data protection issues (*www.ico.org.uk*). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

Cookie Policy

Cookies are very small text files that are stored on your computer when you visit some websites. We use cookies to help identify your computer so we can tailor your user experience and remember where you are in the application process. You can disable any cookies already stored on your computer, but these may stop our website from functioning properly. We will not share any cookie data with any 3rd parties.

Our cookie will:

- Remember whether you are logged in or not, for the duration of your session.
- Remember some limited view and filter preferences.

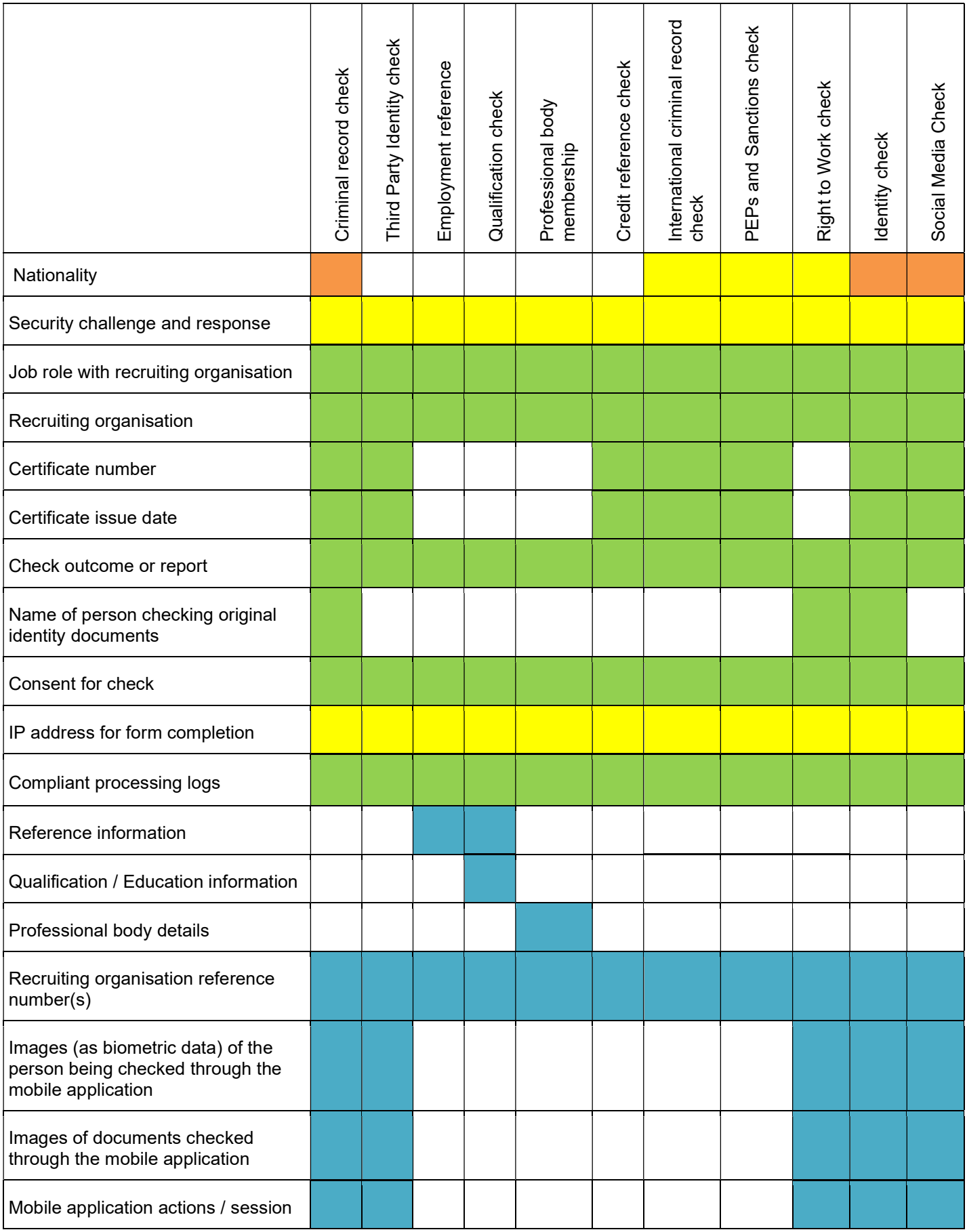
Our cookie will not:

- Remember any form data.

Data Retention Matrix

	Not routinely collected for this product type
	Retained indefinitely if still required by controller or for 7/15 years (in line with DBS retention)
	Retained for 30 days (DBS form data) / 90 days (other data) from result issue (or outcome of a dispute process)
	Retained until data controller withdraws
	Retained as per green (above) unless data subject requests deletion via the controller
	Regulatory body specific retention requirements (please see above)

	Criminal record check	Third Party Identity check	Employment reference	Qualification check	Professional body membership	Credit reference check	International criminal record check	PEPs and Sanctions check	Right to work check	Identity check	Social Media check
Title											
Forename(s)											
Surname(s)											
Date of Birth											
Gender											
Telephone number(s)											
Email address											
Current Address(s)											
Address History											
Name History											
National Insurance Number											
Passport Information											
Driving Licence details											
Additional identity document details											
Birth Country											


Criminal record check
Third Party Identity check
Employment reference
Qualification check
Professional body membership
Credit reference check
International criminal record check
PEPs and Sanctions check
Right to Work check
Identity check
Social Media Check
Nationality
Security challenge and response
Job role with recruiting organisation
Recruiting organisation
Certificate number
Certificate issue date
Check outcome or report
Name of person checking original identity documents
Consent for check
IP address for form completion
Compliant processing logs
Reference information
Qualification / Education information
Professional body details
Recruiting organisation reference number(s)
Images (as biometric data) of the person being checked through the mobile application
Images of documents checked through the mobile application
Mobile application actions / session

Additional usernames or online presence information											